PT0-001 Q&As

CompTIA PenTest+ Exam

Pass CompTIA PT0-001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/pt0-001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A penetration tester has SSH access to a Linux server that is exposed to the internet and has access to a corporate internal network. This server, with IP address 200.111.111.9, only has port TCP 22 externally opened. The penetration tester also discovered the internal IP address 192.168.1.5 from a Windows server. Which of the following steps should the penetration tester follow to open an RDP connection to this Windows server and to try to log on?

A. Connect to the Linux server using # ssh 200.111.111.9, establish an RDP connection to the 192.168.1.5 address.

B. Connect to the Windows server using # ssh -L 3389:200.111.111.9:22 192.168.1.5.

C. Connect to the Linux server using # ssh -L 3389:192.168.1.5:3389 200 .111.111.9; RDP to localhost address, port 3389.

D. Connect to the Windows server using # ssh -L 22:200.111.111.9:3389 192.168.1.5.

Correct Answer: A

QUESTION 2

A penetration tester used an ASP.NET web shell to gain access to a web application, which allowed the tester to pivot in the corporate network. Which of the following is the MOST important follow-up activity to complete after the tester delivers the report?

A. Removing shells

B. Obtaining client acceptance

C. Removing tester-created credentials

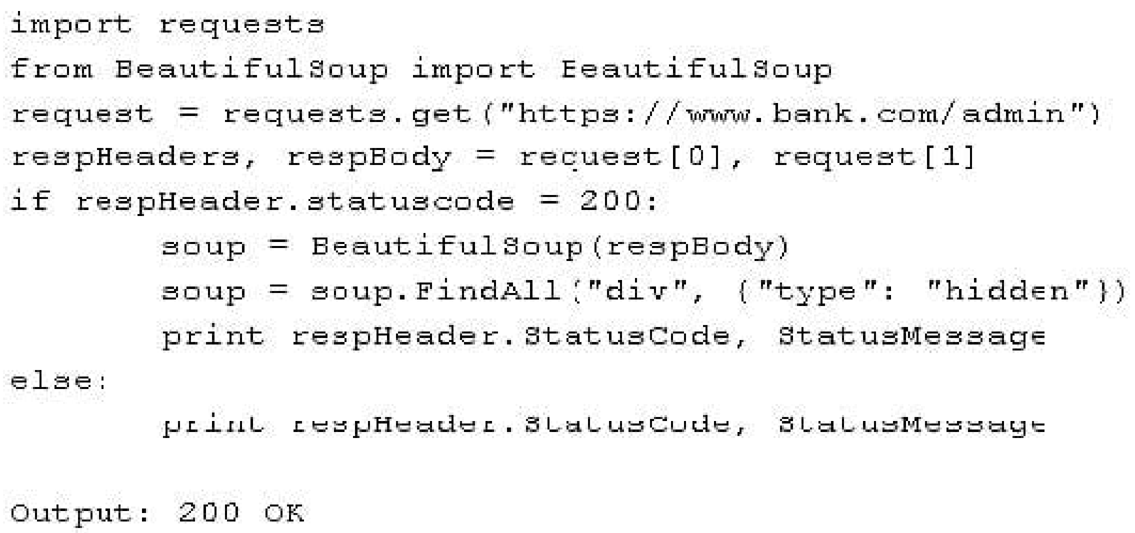
D. Documenting lessons learned

E. Presenting attestation of findings

Correct Answer: E

QUESTION 3

A penetration tester is performing a black box assessment on a web-based banking application. The tester was only provided with a URL to the login page. Given the below code and output: Which of the following is the tester intending to do?



```
import requests
from BeautifulSoup import BeautifulSoup
request = requests.get("https://www.bank.com/admin")
respHeaders, respBody = request[0], request[1]
if respHeader.statuscode = 200:
        soup = BeautifulSoup(respBody)
        soup = soup.FindAll("div", {"type": "hidden"})
        print respHeader.StatusCode, StatusMessage
else:
        print respHeader.StatusCode, StatusMessage

Output: 200 OK
```

A. Horizontally escalate privileges

B. Scrape the page for hidden fields

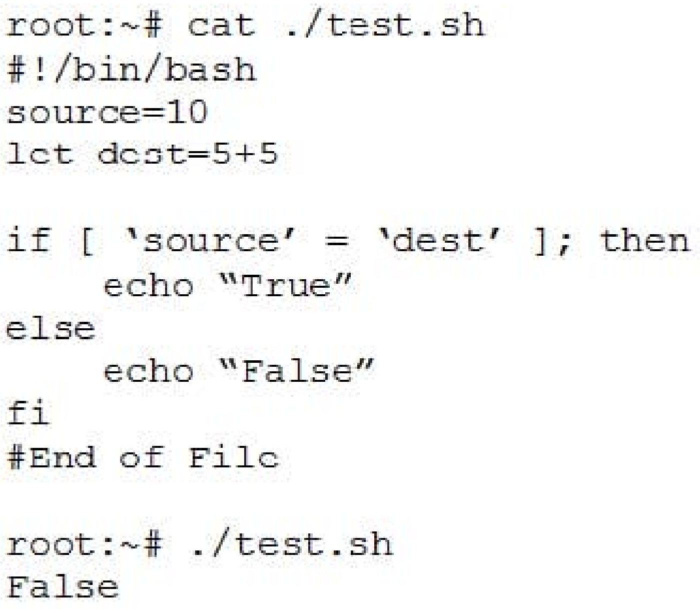
C. Analyze HTTP respond code

D. Search for HTTP headers

Correct Answer: D

QUESTION 4

A penetration tester is checking a script to determine why some basic math errors are persisting. The expected result was the program outputting “True”.



```
root:~# cat ./test.sh
#!/bin/bash
source=10
lct dcst=5+5

if [ 'source' = 'dest' ]; then
    echo "True"
else
    echo "False"
fi
#End of Filc

root:~# ./test.sh
False
```

Given the output from the console above, which of the following explains how to correct the errors in the script? (Choose two.)

A. Change fi\\' to \\'Endlf

B. Remove the \\'let\\' in front of \\'dest=5+5\\'.

C. Change the \\'=" to \\'-eq\\'.

D. Change -Source* and \\'dest\\' to "Ssource" and "Sdest"

E. Change \\'else\\' to \\'elif.

Correct Answer: BD

QUESTION 5

In which of the following scenarios would a tester perform a Kerberoasting attack?

A. The tester has compromised a Windows device and dumps the LSA secrets.

B. The tester needs to retrieve the SAM database and crack the password hashes.

C. The tester has compromised a limited-privilege user and needs to target other accounts for lateral movement.

D. The tester has compromised an account and needs to dump hashes and plaintext passwords from the system.

Correct Answer: C